L. P. USOLTSEV

MATHEMATICS

1962

SovietRxiv

Abstract

Full Text

L. P. USOLTSEV

ESTIMATES OF LARGE DEVIATIONS IN SOME PROBLEMS ON AN INCOMPLETE SYSTEM OF RESIDUES

(Presented by Academician I. M. Vinogradov, November 17, 1961)

MATHEMATICS

In the present paper we solve two problems on estimating large deviations in metric theorems for an incomplete system of residues.

Davenport and Erdős ([1]) proved the following theorem.

Theorem. Let p run through an increasing sequence of primes, beginning with $p = 3$. Let $\left(\frac{m}{p}\right)$, $m = 0, \dots, p-1$, be the Legendre symbol. Extend the definition of the function $\left(\frac{m}{p}\right)$ to all integers m so that it is periodic with period p. Let $h = h(p)$ be an integer-valued function of p such that, as $p \to \infty$, $h \to \infty$ and $\log h / \log p \to 0$. By $N_p(\lambda)$ we shall denote the number of integers a, $0 \le a \le p-1$, for which

$$\frac{1}{\sqrt{h}} \sum_{x=1}^{h} \left(\frac{a+x}{p}\right) < \lambda,$$

where λ is a fixed real number. Then, as $p \to \infty$,

$$\lim_{p\to\infty} \frac{1}{p} N_p(\lambda) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} e^{-z^2/2}\, dz.$$

The question arises of the behavior of the quantity $\frac{1}{p} N_p(\lambda)$ in the case when $\lambda \to \infty$ together with the increase of h. The following theorem holds.

Theorem 1. Let p be an odd prime, and let $h \ge 5$ be an integer such that $h^h \le p^{1/2-\varepsilon}$, where $0 < \varepsilon < \frac{1}{2}$ is a fixed real number. Let $\lambda = \lambda(h)$ be a real-valued function of h such that $\lambda \to \infty$ as $h \to \infty$ and $\lambda \le \sqrt{h}$. By $M_p(\lambda)$ we shall denote the number of integers a, $0 \le a \le p-1$, for which

$$\frac{1}{\sqrt{h}} \sum_{x=1}^{h} \left(\frac{a+x}{p}\right) > \lambda.$$

Then, for $p \ge 2^{1/\varepsilon}$,

$$\frac{1}{p}M_p(\lambda) \le 32e^{-\lambda^2/4}.$$

Proof. Consider the expression

$$v_n = \frac{1}{p}\sum_{a=0}^{p-1}\left(\frac{1}{\sqrt{h}}\sum_{x=1}^{h}\left(\frac{a+x}{p}\right)\right)^{2n} = \frac{1}{h^n}\sum_{x_1=1}^{h}\cdots\sum_{x_{2n}=1}^{h}\frac{1}{p}\sum_{a=0}^{p-1}\left(\frac{(a+x_1)\cdots(a+x_{2n})}{p}\right).$$

If the polynomial $f(a) = (a+x_1)\cdots(a+x_{2n})$ is not congruent modulo p to the square of any polynomial, then, by A. Weil' s theorem ([2]), we have:

$$\left|\sum_{a=0}^{p-1}\left(\frac{(a+x_1)\cdots(a+x_{2n})}{p}\right)\right| \le 4n\sqrt{p}. \qquad (1)$$

Repeating the arguments of Davenport and Erdős ([1]), but taking (1) into account, we obtain

$$v_n = \frac{(2n)!}{n!2^n}\left(1-\frac{\theta_1 n}{p}\right)\left(1-\frac{\theta_2 n}{h}\right)^n + \theta_3\frac{4nh^n}{\sqrt{p}},$$

where $|\theta_1| \leqslant 1,\ |\theta_2| \leqslant 1,\ |\theta_3| \leqslant 1.$ Taking $n_0 = h-1$, for all $n \leqslant n_0$ we obtain

$$v_n \leqslant \frac{(2n)!}{n!2^n}\cdot 2\cdot 2^n + \frac{4}{p^\varepsilon} \leqslant 2\frac{(2n)!}{n!} + 2 \leqslant 4\frac{(2n)!}{n!}.$$

Next consider, for real α, $\alpha^2 \leqslant h/4$, the expression

$$R(\alpha) = \frac{1}{2p}\sum_{a=0}^{p-1}\left(\exp\left[\alpha\frac{1}{\sqrt{h}}\sum_{x=1}^{h}\left(\frac{a+x}{p}\right)\right] + \exp\left[-\alpha\frac{1}{\sqrt{h}}\sum_{x=1}^{h}\left(\frac{a+x}{p}\right)\right]\right).$$

We have:

$$R(\alpha) = \sum_{n=0}^{\infty}\frac{\alpha^{2n}}{(2n)!}\left(\frac{1}{p}\sum_{a=0}^{p-1}\left(\frac{1}{\sqrt{h}}\sum_{x=1}^{h}\left(\frac{a+x}{p}\right)\right)^{2n}\right).$$

Let us estimate $R(\alpha)$ from above. Since $\alpha^2 \leqslant h/4$, $n_0 = h-1$, $h \geqslant 5$, $n_0! \geqslant (n_0/3)^{n_0}$, we have $\alpha^{2n_0}/n_0! \leqslant (15/16)^4$ and

$$1+\frac{\alpha^{2n_0}}{n_0!}+\left(\frac{\alpha^{2n_0}}{n_0!}\right)^2+\cdots\leqslant 4,$$

whence

$$R(\alpha)=\sum_{n=0}^{\infty}\frac{\alpha^{2n}}{(2n)!}\,v_n\leqslant$$

$$\leqslant\sum_{n=0}^{n_0-1}\frac{\alpha^{2n}}{(2n)!}v_n+\frac{\alpha^{2n_0}}{(2n_0)!}v_n\sum_{n=0}^{n_0-1}\frac{\alpha^{2n}}{(2n)!}v_n+\left(\frac{\alpha^{2n_0}}{(2n_0)!}v_{n_0}\right)^2\sum_{n=0}^{n_0-1}\frac{\alpha^{2n}}{(2n)!}v_n+\cdots\leqslant$$

$$\cdots\leqslant\left\{1+\frac{\alpha^{2n_0}}{(2n_0)!}v_{n_0}+\left(\frac{\alpha^{2n_0}}{(2n_0)!}v_{n_0}\right)^2+\cdots\right\}\sum_{n=0}^{n_0-1}\frac{\alpha^{2n}}{(2n)!}v_n\leqslant 16e^{\alpha^2}.$$

Let us estimate $R(\alpha)$ from below.

$$R(\alpha)\geqslant\sum_{n=0}^{\infty}\frac{\alpha^{2n}}{(2n)!}\lambda^{2n}\frac{1}{p}M_p(\lambda)=\frac{1}{p}M_p(\lambda)\sum_{n=0}^{\infty}\frac{(\alpha\lambda)^{2n}}{(2n)!}\geqslant\frac{e^{|\alpha|\lambda}}{2}\,\frac{1}{p}M_p(\lambda).$$

Comparing the lower and upper estimates for $R(\alpha)$, we obtain:

$$\frac{1}{p}M_p(\lambda)\leqslant 32e^{\alpha^2-|\alpha|\lambda}.$$

Take $\alpha=\lambda/2$, which does not contradict the condition $\alpha^2\leqslant h/4$, since $\lambda=\sqrt{h}$. We obtain $\frac{1}{p}M_p(\lambda)\leqslant 32e^{-\lambda^2/4}$. The theorem is proved.

The work of Davenport and Erdős was generalized by I. P. Kubilius and Yu. V. Linnik ([3]). The arguments of Theorem 1 can without difficulty be extended also to the case studied by I. P. Kubilius and Yu. V. Linnik.

A. G. Postnikov ([4]) proved the following theorem.

Theorem. Let $g\geqslant 2$ be a natural number. Let p run through a sequence of primes, $h=h(p)$ an integer-valued function of p

such that $h\to\infty$ as $p\to\infty$ and

$$h\leqslant\frac{1}{p}\frac{\log p}{\log g}.$$

By $N_p(\lambda)$ we shall denote the number of integers a, $0\leqslant a\leqslant p-1$, for which

$$\frac{1}{\sqrt{h}}\left|\sum_{x=1}^{h} e^{2\pi i \frac{ag^x}{p}}\right| < \lambda,$$

where $\lambda > 0$ is a fixed real number. Then, as $p \to \infty$,

$$\lim_{p\to\infty} \frac{1}{p} N_p(\lambda) = 1 - e^{-\lambda^2}.$$

Here, as above, in the problem of Davenport and Erdős, the question arises of the behavior of the quantity $\frac{1}{p}N_p(\lambda)$ in the case when $\lambda \to \infty$ together with the increase of h. The following theorem is true.

Theorem 2. Let $g \geqslant 2$ be a natural number; let $0 < \eta < 1$ be a real number; let p be a prime number; and let h be a natural number such that

$$h \leqslant (1-\eta)\frac{\log p}{\log g}.$$

Denote by $M_p(\lambda)$ the number of integers a, $0 \leqslant a \leqslant p-1$, for which

$$\frac{1}{\sqrt{h}}\left|\sum_{x=1}^{h} e^{2\pi i \frac{ag^x}{p}}\right| > \lambda,$$

where $\lambda = \lambda(h) \geqslant 2$ is an arbitrary real function. Then

$$\frac{1}{p} M_p(\lambda) \leqslant \frac{3\lambda^2}{2} e^{-\lambda^2/4}.$$

Proof. It is easy to prove that the number of representations of a natural number N in the form

$$N = g^{x_1} + \ldots + g^{x_n},$$

where x_i $(i = 1, \ldots, n)$ are natural numbers, does not exceed $3^n n!$, whence it follows that the number of solutions $A_n(h)$ of the equation

$$g^{x_1} + \ldots + g^{x_n} = g^{y_1} + \ldots + g^{y_n}$$

in integers $1 \leqslant x_i, y_j \leqslant h$ $(i, j = 1, \ldots, n)$ does not exceed $3^n n!\, h^n$.

For positive $s \geqslant 1$, consider the expression

$$R(s) = \frac{1}{2p}\sum_{a=0}^{p-1}\left(\exp\left[-s\frac{1}{\sqrt{h}}\left|\sum_{x=1}^{h} e^{2\pi i\frac{ag^x}{p}}\right|\right] + \exp\left[s\frac{1}{\sqrt{h}}\left|\sum_{x=1}^{h} e^{2\pi i\frac{ag^x}{p}}\right|\right]\right).$$

We have:

$$R(s) = \sum_{n=0}^{\infty}\frac{s^{2n}}{(2n)!}\left(\frac{1}{p}\sum_{a=0}^{p-1}\left(\frac{1}{\sqrt{h}}\left|\sum_{x=1}^{h} e^{2\pi i\frac{ag^x}{p}}\right|\right)^{2n}\right).$$

Let us estimate $R(s)$ from above. Since from

$$2^n = (1+1)^n \leqslant \frac{(2n)!(2n+1)}{(n!)^2}$$

it follows that

$$\frac{2^{2n}n!}{(2n)!} \leqslant \frac{2n+1}{n!},$$

and since, according to (4),

$$\frac{1}{p}\sum_{a=0}^{p-1}\left(\frac{1}{\sqrt{h}}\left|\sum_{x=1}^{h} e^{2\pi i\frac{ag^x}{p}}\right|\right)^{2n} = \frac{A_n(h)}{h^n},$$

then

$$R(s) = \sum_{n=0}^{\infty}\frac{s^{2n}}{(2n)!}\frac{A_n(h)}{h^n} \ll \sum_{n=0}^{\infty}\frac{s^{2n}3^n n!}{(2n)!} \ll \sum_{n=0}^{\infty}\frac{s^{2n}2^{2n}n!}{(2n)!} \ll$$

$$\ll \sum_{n=0}^{\infty}\frac{s^{2n}(2n+1)}{n!} = \left(\sum_{n=0}^{\infty}\frac{s^{2n+1}}{n!}\right)' = (se^{s^2})' = (2s^2+1)e^{s^2} \leq 3s^2e^{s^2}.$$

Let us estimate $R(s)$ from below:

$$R(s) \gg \sum_{n=0}^{\infty}\frac{s^{2n}}{(2n)!}\frac{1}{p}M_p(\lambda)\lambda^{2n} = \frac{1}{p}M_p(\lambda)\sum_{n=0}^{\infty}\frac{(s\lambda)^{2n}}{(2n)!} =$$

$$= \frac{1}{p}M_p(\lambda)\frac{e^{-s\lambda}+e^{s\lambda}}{2} \geq \frac{e^{s\lambda}}{2}\frac{1}{p}M_p(\lambda).$$

Comparing the upper and lower estimates for $R(s)$, we obtain:

$$\frac{1}{p}M_p(\lambda) \ll \frac{6s^2 e^{s^2}}{e^{s\lambda}}.$$

Taking $s = \lambda/2$ (which does not contradict the condition $s \geq 1$, since $\lambda \geq 2$), we obtain:

$$\frac{1}{p}M_p(\lambda) \ll \frac{3\lambda^2}{2} e^{-\lambda^2/4}.$$

The theorem is proved.

I express my gratitude to Yu. I. Manin for a valuable consultation.

Mathematical Institute named after V. A. Steklov
Academy of Sciences of the USSR

Received
9 XI 1961

REFERENCES CITED

1. H. Davenport, P. Erdös, Publ. Math., **2**, 252 (1952).
2. A. Weil, Proc. Nat. Acad. Sci., **34**, 204 (1948).
3. I. P. Kubilyus, Yu. V. Linnik, Izv. Vyssh. uchebn. zaved., ser. matem., No. 6 (13), 88 (1959).
4. A. G. Postnikov, DAN, **133**, No. 6, 1298 (1960).

Note: Figure translations are in progress. See original paper for figures.